Program Protection Plan Outline & Guidance

• VERSION 1.0 •

• July 2011 •

Tailored for Defense Business Systems (June 13, 2013)

Deputy Assistant Secretary of Defense

Systems Engineering

Introduction

This document provides an outline, content, and formatting guidance for the Program Protection Plan (PPP) required by DoDI 5000.02 and DoDI 5200.39.

This version of the PPP outline dated June 2013 has been tailored for the Defense Business Systems. The tailoring includes removal of CPI, anti-tamper, defense exportability features, program protection costs, counterintelligence plan, horizontal protection, and ASDB, because DBS use commercial technology. This plan is predicated on a successful IA certification and accreditation.

General Guidance:

- Program Protection is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.
- The purpose of the PPP is to help programs ensure that they adequately protect their technology, components, and information. This includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, or defeat warfighting capability.
- The process of preparing a PPP is intended to help program offices consciously think through what needs to be protected and to develop a plan to provide that protection. Once a PPP is in place, it should guide program office security measures and be updated as threats and vulnerabilities change or are better understood.
- It is important that an end-to-end system view be taken when developing and executing the PPP. External, interdependent, or government furnished components that may be outside a program managers' control must be considered.
- The Acquisition Information Assurance (IA) Strategy must be appended to the PPP. Wherever possible, reference or point to other documents containing relevant information rather than duplicating the information in the PPP unless that information would be valuable to users of the plan. Do not simply repeat general policies unless that information would be valuable to the user of the plan.

The office of primary responsibility for this guide is the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). This office will continue to develop and coordinate updates to the guide as required, based on any future policy changes and customer feedback. To provide feedback, send e-mail to dasd-se@osd.mil.

[PROGRAM NAME] – [ACAT LEVEL]

PROGRAM PROTECTION PLAN
VERSION [#]

SUPPORTING MILESTONE [MS] AND
[APPROPRIATE PHASE NAME]

[DATE]

****

_____ _____

Undersecretary of Defense
Acquisition, Technology, and Logistics
[or appropriate Milestone Decision Authority for non-ACAT ID programs]

Date

SUBMITTED BY

_____ _____

Name
Program Manager

Date

CONCURRENCE

_____ _____

Name
Program Executive Officer or
Equivalent

Date

COMPONENT APPROVAL
[Required for programs with OSD approval (ACAT ID, IAM, etc.)]

_____ _____

Name
Component Acquisition Executive

Date

Contents

1.0. Introduction – Purpose and Update Plan

- Who will use the PPP?
- What aspects of Program Protection will you ask the contractor to do?
- Summarize how the PPP will be updated and the criteria for doing so to include:
    - Timing of PPP updates (e.g. prior to milestone, , following a major enhancement),
    - Update authority
    - Approval authority for different updates

Table 1.0-1 PPP Update Record (mandated)

Revision Number	Date	Changes	Approved By

1.1. Program Protection Responsibilities

- Who is responsible for Program Protection on the program?
- Include contact information for Program Protection leads/resources/SMEs.
- For every countermeasure being implemented, identify who is responsible for execution.

Table 1.2-1: Program Protection Responsibilities (mandated) (sample)

Title/Role	Name	Location	Contact Info
Program Manager			
Lead Systems Engineer			
Program Protection Lead			
Info. Assurance Lead			
Software Assurance Lead			
SCRM Lead			
…			

2.0. Program Protection Summary

2.1. Schedule

- A Program Protection schedule overlaid onto the program's master schedule (milestones, systems engineering technical reviews, etc.) includes:
    - Critical function/component identification/updates
    - Threat assessment requests
    - Vulnerability assessments, red teams, etc.
    - Security Audits/Inspections
    - Engagement with Systems Engineering Technical Reviews (e.g. subsystem Preliminary Design Reviews for critical components)
    - Countermeasure (e.g. Software Assurance, Information Assurance) testing/verification events
    - Foreign involvement events (Exportability likelihood assessment, Cooperative Development, License Requests, etc.)

Expectation: Program Protection activities and events should be integrated in overall program scheduling.

2.2. Critical Functions and Components Protection

- Clearly articulate that the program does not contain CPI.
- Over the lifecycle of the program list all critical functions and components (including inherited and organic) mapped to the security disciplines of the countermeasures being applied in Table 2.2-1 below.
- For each countermeasure being implemented, list who is responsible for execution in Section 1 above.
- Table 2.2-1 is meant to summarize the protection scheme/plan for the program. The detail supporting this summary assessment (including the threats and vulnerabilities the selected countermeasures apply to) is planned for and documented in the subsequent sections of the document.

Table 2.2-1: Critical Components Countermeasure Summary (mandated) (sample)

	#	Protected Item (Inherited and Organic)	Countermeasures															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Critical Components	7	iDirect M1D1T Hub-Line Card	X	X	X	X	X	X	X	X				X	X	X		
	8	Cisco Router IOS with Advance Security Option (ASO)	X	X	X	X	X	X								X		
	9																	
	10																	

KEY *[Examples Included: UPDATE THIS LIST ACCORDING TO PROGRAM]*			
	General CMs	**Research and Technology Protection CMS**	**Trusted Systems Design CMs**
Key **X =** Implemented	**1** Personnel Security **2** Physical Security **3** Operations Security **4** Industrial Security **5** Training **6** Information Security **7** Foreign Disclosure/Agreement	**8** Transportation Mgmt **9** Dial-down Functionality	**11** IA/Network Security **12** Communication Security **13** Software Assurance **14** Supply Chain Risk Management **15** System Security Engineering (SSE) **16** Other

3.0. Critical Components

3.1. Identification Methodology

Describe the methodology that will be used to identify mission critical functions and components in accordance with DoDI 5200.39[1] and DoDI 5000.02[2]. Include:

- Criticality analysis participants
- Timing of identification and updates to mission critical functions and components
- Approach for performing criticality analysis

Expectations: The end-to-end system must *b*e considered, including items such as mission packages, government furnished components, and interdependent systems that may be outside a program manager's control. Mission critical functions and components must be identified by a multi-disciplined group. Criticality analysis should be led by systems engineers and mission/operator representatives. Information regarding these components and/or technologies must be considered for protection. Criticality analysis updates should be tied to Systems Engineering Technical Reviews. Early in the program this section will reflect intentions, in updates it will provide a record of what has been done and any remaining work.

3.2. Inherited Critical Components

For any critical components identified, summarize the approach to identifying and managing Program Protection risks.

- Identify the system the inherited item comes from. Will it be protected in the same way it was originally? Indicate variances in usage and plans for adjusting countermeasures as appropriate
- Identify the POC for answering questions about the inherited system(s). How will the program interact with them to ensure awareness of inherited threats, vulnerabilities, countermeasures, and risks?
- Consider enabling or supporting services and infrastructure functions provided by other programs or agencies (e.g., Data centers, Clouds, Enterprise Service, ERP backbone)

Table 3.2-1: Inherited Critical Components (mandated)

	Inherited Critical Item	Parent Program	Original Use	Planned Use	Variation in CMs?	Inherited Program POC
Critical Components						

[1] http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf
[2] http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

3.3. Organic Critical Components

As Critical Components are identified, track them in Table 3.3-1 below.

- Identify critical components, and summarize the effects or consequences if they are compromised. Track any adds/changes/deletions from this list over the course of the program with rationale for the edit.
- Where will the critical components be physically located during the acquisition lifecycle? Indicate whether or not contractor PPIPs are in place to flow protection requirements to contractor locations.
- Show traceability from mission-level documents (Business Need/Case, Business Enterprise Architecture, JCIDS Key Performance Parameters, Key System Attributes, etc.) and Critical Technology Elements (CTE) to the system architecture.

Table 3.3-1: Organic Critical Components (mandated)

	Assessment Date(s): 22 December 2009							
	CC	**Consequence of Compromise**	**Status/ Date & Justification for Status Change**		**Traceable CTEs, KPPs, etc.**	**Export Control Areas**	**Physical Location**	**System Location PPIP Exists?**
Critical Components								

4.0. Threats, Vulnerabilities, and Countermeasures

- Summarize any identified threats and vulnerabilities to critical functions/components in Table 4.0-1 below. Also identify any countermeasures selected to mitigate risks of compromise.
- This table should be updated over time as the information is identified; early in the program, identify the plan for obtaining this information in Sections 4.1-4.3 below.
- The numbers in the threat and vulnerabilities tables should correspond to the numbered rows in the threat table (4.1-2) and vulnerability table (4.2-1) below. All critical functions/components should be reflected in the table.

Table 4.0-1: Summary of Threat, Vulnerabilities, and Countermeasures (mandated) (sample)

	CC (and CC supplier) Section 2.0	**Threats** Section 5.1	**Vulnerabilities** Section 5.2	**Countermeasures** Section 5.3
Critical Components	iDirect M1D1T Hub-line Card	2, 8, 9, 14	3	Communication Security; Software Assurance; SCRM
	Cisco Router IOS with ASO	2, 6, 8, 9, 14	4	Supply Chain Risk Management

4.1. Threats

- Who is responsible for requesting and receiving threat products, and when will they be requested? Who in the intelligence community is responsible for supporting these requests? Include these contacts in the table in Section 1.2.
- What threat products will be requested for the program, when, and how will they be used?
- How frequently will threat products be updated?
- For threat products that have been received, what threats were identified?

Table 4.1-1: Threat Product References (mandated) (sample)

Title of Program-Specific or Other Threat Products Used for PPP Threat Analysis	Classification	Document Date	Organization(s) Producing the Product	Reference/ Link to Product
Formal Threat Reports				
Capstone Threat Assessment (CTA)	U-S	Dec 2002	Defense Intelligence Agency	
System Threat Assessment Report (STAR)	S	Jan 2007	Defense Intelligence Agency	
Supply Chain Threat Assessments				
iDirect M1D1T Hub-line Card Assessment	TS/SCI	Apr 2009	Defense Intelligence Agency	
Cisco Router IOS with ASO	TS/SCI	Apr 2009	Defense Intelligence Agency	
Other Threat Documents				
Technology Collection Trends in the U.S. Defense Industry	U	Oct 2006	Defense Security Service	
Targeting U.S. Technologies	U	Feb 2007	Defense Security Service	

Expectations: As threat products are received, reference these documents in Table 4.1-1. For the Supply Chain Threat Assessments, document each critical component supplier (or potential supplier) that has been assessed. Summarize the threats identified in Table 4.1-2 below.

Table 4.1-2: Identified Threats (mandated) (sample)

T#	Threat	Description	Consequence of threat realization
1	Malicious Code Insertion	Country Y is known to have inserted malware into the software that Critical Component #2 depends on	Degraded or untrustworthy performance of targeting module
2			
3			

4.2. Vulnerabilities

- What vulnerabilities have been identified to date?
- How will the program identify new vulnerabilities (both system-level and in the development environment) to the mission-critical functions and components? Who is responsible for doing this, and with what frequency? Include the responsible person in the table in Section 1.2.
- How often will vulnerabilities be re-assessed?
- How will identified vulnerabilities be mitigated?
- Summarize the results of any vulnerability assessments, red teams, etc. performed to date in Table 4.2-1 below.

Table 4.2-1: Potential Critical Component Vulnerabilities (mandated)

V#	Critical Components	Identified Vulnerabilities

1		
2		
3		

4.3. Countermeasures

- How will countermeasures be selected to protect critical functions/components? Who has the responsibility for their implementation? Include in the table in Section 1.2.
- How will contracts supporting the acquisition program incorporate protection requirements? Indicate the RFP Contract Line Item Number (CLIN) or Data Item Description (DID) that will be used to ensure that critical functions/components are protected in the development environment and on the system
- Succinctly describe the implementation of each countermeasure used to protect critical functions and components. Be specific: If SCRM Key Practices apply, describe which ones; if using Software Assurance techniques, explain which ones.
- Indicate planned implementation and actual implementation as the PPP evolves. Explain deviations from the plan.
- At a minimum, address implementation of the countermeasures in Section 4.3.1- 4.3.5 or rationale for not using them:

4.3.1. Information Assurance (IA)

- Who is responsible for assessing the adequacy of IA countermeasures for critical functions and components?? What are the key IA schedule milestones?
- How will the appropriate implementation of IA protections for DoD information systems (other than the system being acquired) hosting critical functions and components be ensured?
- How will the appropriate implementation of IA protections for contractor-owned information systems (or other non-DoD information systems) hosting critical functions and components be ensured?
    - How will IA controls be negotiated with contractors?
    - Who will ensure these controls are flowed down to subcontractors?
    - Who will keep an inventory of critical functions and components hosted on contractor information systems?
- How will the appropriate implementation of IA protections for the system being acquired be ensured?
    - Include the Component CIO approved Acquisition IA Strategy as an Appendix. (See Appendix E description in this document)

Expectation: IA countermeasures planning should account for the system being acquired and any support information systems that may contain or host critical functions and components. The Acquisition IA Strategy documents the plan for implementing IA specifically on the system being acquired. IA controls can also be applied to protect critical functions and components as they are handled/transmitted across contractor or partner systems. For example, contractor

development environments may host critical components and should be evaluated for protection.

4.3.2. Software Assurance

- Who is responsible for Software Assurance?
- How will software be designed and tested to assure protection of critical functionality?
    - How will software architectures, environments, designs, and code be evaluated with respect to CVE (Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification), and CWE (Common Weakness Enumeration)?
        - CVE – Used to identify and coordinate SW vulnerabilities that enable various types of attacks.
        - CAPEC – Used for the analysis of common destructive attack patterns
        - CWE – Used to examine software architecture/design and source code for weaknesses.
- How will COTS software and software of unknown pedigree (i.e., software from sources buried in the supply chain) be protected and tested/vetted?
- How will the critical functions be protected in the operational system?
- How will the development environment be protected?
    - List the development environment tools
- Who has access to the development environment?
    - Who will be responsible for maintaining a list of cleared, US citizens as well as foreign nations/nationals that have access?
    - Where will the list be stored, and how often will it be updated?
- P/A indicates planned/actual – explain any deviations from planned testing/evaluation rates. For further details see key practices 9, 11, 16,17,19,21 and 23 in the "Key Practices and Implementation Guide for DOD Comprehensive National Cyber Initiative 11 Supply Chain Risk Management Pilot Program."

Table 4.3.3-1: Application of Software Assurance Countermeasures (sample)

Development Process								
Software (Critical function components, other software)	**Static Analysis p/a (%)**	**Design Inspect**	**Code Inspect p/a (%)**	**CVE p/a (%)**	**CAPEC p/a (%)**	**CWE p/a (%)**	**Pen Test**	**Test Coverage p/a (%)**
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25
COTS Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK
Operational System								
	Failover Multiple Supplier	**Fault Isolation**	**Least Privilege**	**System Element Isolation**		**Input checking / validation**		**SW load key**

	Redundancy (%)					
Developmental Critical Function SW	50	All	All	yes	All	all
Other Developmental SW	none	Partial	none	None	all	all
COTS (CF) and NDI SW	none	Partial	All	None	Wrappers/ all	all

Development Environment								
SW Product	**Source**	**Release testing**	**Generated code inspection p/a (%)**					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment Access	Controlled access; Cleared personnel only							

4.3.3. Supply Chain Risk Management

- How will the program manage supply chain risks to critical functions and components?
- Explain how supply chain threat assessments will be used to influence system design, development environment, and procurement practices. Who has this responsibility? When will threat assessments be requested?

4.3.3.1.Counterfeit Prevention

- What counterfeit prevention measures will be in place? How will the program mitigate the risk of counterfeit insertion during Operations and Maintenance?

4.3.4. General Countermeasures

- Summarize generic countermeasures or security activities in place that will/do apply to all program information/facilities/personnel and contribute to the protection of critical functions and components.

Table 4.3.6-1: Generic Program Countermeasures/Security Activities (mandated) (sample)

Type	**Detail**
COMSEC (Development Environment)	• Program Office Policy XX-XXX details program COMSEC countermeasures that are implemented at each government facility.
OPSEC	• Program Management Directive XX-XXX, will be tailored to satisfy specific security requirements of individual PROGRAM XYZ activities. • The PROGRAM XYZ effort will comply fully with AFI 10-701, Operations Security • The 669 AESS OPSEC Plan identifies all PROGRAM XYZ critical information.
Foreign Visit Program	• Program office personnel, other government organizations and contractors will adhere to approved visit procedures for the facility being visited.

Information Assurance (Development Environment)	• Prime Contractor network security architecture and configuration will be managed by the CIO. Network security procedures and countermeasures applicable to subnets containing Government CUI are available upon request. The program will comply with DTM 08-027 "Security of Unclassified DoD Information on Non-DoD Information Systems".
Secure System Administration	• System configuration will be managed remotely by the DISA GNSC/TNC administrators.
Personnel Security	• The 669 AESS/SF is responsible for reviewing personnel security procedures at all 669 AESS and PROGRAM XYZ industry locations. This will be coordinated with DSS for industry reviews.
Industrial Security	• Security protection requirements will be incorporated into all PROGRAM XYZ contracting activities. Government procedures and instructions for preparing DD Forms 254, Contract Security Classification Specifications, will ensure that contractors are provided quality acquisition security, Program Protection, and classification management guidance.

5.0. Other System Security-Related Plans and Documents

- Reference relevant acquisition or system security-related documents.

Table 5.0-1: Other System Security-Related Plans and Documents (mandated) (sample)

Plan	Organization	Link/POC
Test & Evaluation Master Plan	TEMP Approval Authority	
Systems Engineering Plan	SEP Approval Authority	
Software Secure Coding Standards	Contractor SW Design Lead	
Trusted Software Design Techniques	Contractor SW Design Lead	
Secure Software Process Standards	Contractor SW Design Lead	

Expectation: If Technical Assistance Agreements, Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), or other similar agreements have been signed, reference or link to them in an additional table with a description of the key commitments.

6.0. Program Protection Risks

- Describe how Program Protection risks (cost, schedule, technical) will be integrated with overall Program risk management.
- Discuss the approach to identifying residual risks of critical function and component compromise after countermeasure implementation. Are there any unmitigated risks?
- Include a risk cube and mitigation plan for the top Program Protection risks.

7.0. Processes for Management and Implementation of PPP

There are several types of checking PPP implementation. Audits/inspections are used to ensure compliance with applicable laws, regulations, and policies. Engineering reviews are used to ensure that system security requirements are identified, traceable and met throughout the acquisition lifecycle.

7.1. Audits/Inspections

- Summarize the timing of security audits/inspections. How will contractor security requirements be enforced? Who is responsible for this?

7.2. Engineering/Technical Reviews

- How will system security requirements be addressed in Systems Engineering Technical Reviews, functional/physical configuration audits, etc? Who is responsible for this?
- What Program Protection entry/exit criteria will be used for these reviews?

7.3. Verification and Validation

- Explain how the program will integrate system security requirements testing into the overall test and evaluation strategy. Who is responsible for this?
- Link to relevant discussion in T&E documents.

7.4. Sustainment

- How will Program Protection requirements and considerations be managed in sustainment? Who is responsible for this?
- Link to the relevant Lifecycle Sustainment Plan (LCSP) language.

8.0. Processes for Monitoring and Reporting Compromises

- Summarize the plan/procedure for responding to a supply chain exploit.
- What constitutes a compromise or exploit? Who is notified if one occurs? Define what constitutes a Supply Chain exploit.

Appendix A: Security Classification Guide

- *The SCG may be referenced or pointed to rather than included in the document.*

Appendix C: Criticality Analysis

- Document the results of the most recent Criticality analysis in table C-1 below. The CA should be updated regularly (e.g. at each SE Technical Review)
- Early in the program lifecycle, the CA may only be able to identify missions or missions and critical functions.
- Criticality should be assessed in terms of relative impact on the system's ability to complete its mission if the component fails. Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible.

•

Table C-1: Criticality analysis Part 1 - Missions, Functions, and Components

Missions	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I, II, III, IV)
Mission 1	Data Fusion	Processor X	II
		SW Module Y	I
	Fire Control	Database Z	III
		SW Module A	I
	Critical Function 3	Processor X	II
		Sensor A	IV
Mission 2	Critical Function 4	Sensor B	I
		Radar A	I
	Critical Function 5	Processor Y	II
		SW Module B	II
	Critical Function 6	Database Y	III
		Integrated Circuit A	I
Mission 3	Data Fusion	Processor X	II
		SW Module Y	I

The Level I and Level II components identified in Table C-1 were then prioritized for resources and attention based on a variety of factors.

Appendix E: Information Assurance Strategy

Foreword

1. The reuse of existing documentation in preparing the acquisition IA strategy document is strongly encouraged where practicable. For example, the integrated schedule in the program's approved acquisition strategy may be referenced in the "program information" section. However, it is incumbent on the submitting PMO to ensure that any such information is readily available to the document review/approval chain by providing copies of the referenced documents in conjunction with the acquisition IA strategy document. References to draft documents are not sufficient to support approval of the acquisition IA strategy document.
2. In consideration of the different levels of maturity relative to acquisition phases, and to encourage brevity and focus, the following page limitations are imposed:

- Acquisition IA Strategies are not required for Material Development Decisions (MDD)
- Acquisition IA Strategies for Milestone A - 7 pages
- Acquisition IA Strategies for Milestone B or C – 15 pages
- Acquisition IA Strategies for Full Rate Production (FRP) or Full Deployment Decision (FDD) - 15 pages

Tables of content, acronym lists, signature sheets and executive summaries are not required, but if included do not count against the page limitations.
3. As part of the Acquisition Documentation Streamlining effort, DOASD(I&IA) has reached agreement with DASD(SE) proposal that the Acquisition IA Strategy be included as an appendix to the Program Protection Plan. This does not affect the current review and approval process for the Acquisition IA Strategy document, since only documents that have been approved by the Component CIO and reviewed by the DoD CIO (with a formal review report issued by ODASD(I&IA)/DIAP)) will be appended to the PPP.
4. Program offices should utilize the template on the following page in the preparation of their Acquisition IA Strategy documents.
5. IA threats must be included in the PPP threat table.

I. Program and System Description.

A. Program Information (Applicable to MS A, B, C, FRP/FDD)

Identify the Acquisition Category (ACAT) of the program. Identify current acquisition life-cycle phase and next milestone decision. Include a graphic representation of the program's schedule.

B. System Description (Applicable to MS A, B, C, FRP/FDD)

Provide or reference a high-level overview of the specific system being acquired. Characterize the system as to type of DoD information system (AIS application, enclave, platform IT interconnection, outsourced IT-based process), or as Platform IT without a GIG interconnection. Provide or reference a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe or reference the system's function, and summarize significant information exchange requirements and interfaces with other IT or systems, as well as primary databases supported. Identify the primary network(s) to which the system will be connected (e.g. NIPRNET, SIPRNET, JWICS, etc.). Provide a description or graphic defining the system's accreditation boundary.

II. Information Assurance Requirements.

A. Sources (Applicable to MS A, B, C, FRP/FDD)

1. Mission Assurance Category and Confidentiality Level

Identify the system's MAC and Confidentiality Level as specified in the applicable capabilities document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2. If the system architecture includes multiple segments with differing MAC and CL combinations, include a table listing all segments and their associated MAC and CL designations, as well as a brief rationale for the segmentation.

2. Baseline IA Control Sets

Identify the applicable sets of Baseline IA Controls from DoD Instruction 8500.2 that will be implemented. A listing of individual controls is not required.

3. ICD/CDD/CPD specified requirements

List any specific IA requirements identified in the approved governing capability documents (e.g. Initial Capabilities Document, Capability Development Document or Capability Production Document).

4. Other requirements

List any IA requirements specified by other authority (i.e. Component mandated).

B. IA Budget (scope and adequacy) (Applicable to MS A, B, C, FRP/FDD)

Describe how IA requirements for the full life cycle of the system (including costs associated with certification and accreditation activities) are included and visible in the overall program budget. Provide a statement of the adequacy of the IA budget relative to requirements.

III. System IA Approach (high level): (Applicable to MS B, C, FRP/FDD)

A. System IA technical approach

Describe, at a high level, the IA technical approach that will secure the system.

B. Protections provided by external system or infrastructure

List any protection to be provided by external systems or infrastructure (i.e. inherited control solutions).

IV. Acquisition of IA Capabilities and Support: (Applicable to MS B, C, FRP/FDD)

Describe how the program's contracting/procurement approach is structured to ensure each of the following IA requirements are included in system performance and technical specifications, RFPs and contracts (as well as other agreements, such as SLAs, MOAs, etc.) early in the acquisition life cycle.

A. System IA capabilities (COTS or developmental contract)
B. GFE/GFM (external programs)
C. System IA capabilities as services (commercial or government)
D. Information Systems Security Engineering (ISSE) services
E. IA professional support services to the program (commercial or government, including C&A support)

Confirm that program contracts/agreements communicate the requirement for personnel performing IA roles to be trained and appropriately certified in IA in accordance with DoD Directive 8570.01.

V. System Certification and Accreditation:

A. Process (DIACAP; DCID 6/3, etc) (Applicable to MS A, B, C, FRP/FDD)

Identify the specific Certification and Accreditation (C&A) process to be employed (e.g., DoD Information Assurance Certification and Accreditation Process (DIACAP), NSA/CSS Information Systems Certification and Accreditation Process (NISCAP), DoD Intelligence Information System (DODIIS)). If the system being acquired is platform IT without a GIG interconnection, describe any Component level process imposed to allocate and validate IA requirements prior to operation.

B. Key role assignments (Applicable to MS B, C, FRP/FDD)

Provide the name, title, and organization of the Designated Accrediting Authority, Certification Authority, and User Representative for each separately accreditable system being acquired by the program.

C. C&A timeline (Applicable to MS B, C, FRP/FDD)

Provide a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of Interim Authorization to Test (IATT), Interim Authorization to Operate (IATO), and Authorizations to Operate (ATOs). Normally, it is expected that an ATO will be issued prior to operational test and evaluation.

D. C&A approach (Applicable to MS B, C, FRP/FDD)

If the program is pursuing an evolutionary acquisition approach, describe how each increment will be subjected to the certification and accreditation process. If the C&A process has started, identify significant activity completed, and whether an ATO or IATO was issued. If the system being acquired will process, store, or distribute Sensitive Compartmented Information, compliance with Intelligence Community Directive (ICD) 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" is required, and the plan for compliance should be addressed. Do not include reiterations of the generic descriptions of the C&A process (e.g. general descriptions of the DIACAP activities from DoDI 8510.01 and the DIACAP Knowledge Service).

VI. IA Testing:

A. Testing Integration (Applicable to MS A, B, C, FRP/FDD)

Confirm that all IA testing and C&A activities will be/has been integrated into the program's test and evaluation planning, and incorporated into program testing

documentation, such as the Test and Evaluation Strategy and Test and Evaluation Master Plan.

B. Product Evaluation (e.g. IA/IA enabled products) (Applicable to MS B, C, FRP/FDD)

List any planned incorporation of IA products/IA enabled products into the system being acquired, and address any acquisition or testing impacts stemming from compliance with NSTISSP Number 11.

C. Cryptographic Certification (Applicable to MS B, C, FRP/FDD)

List any planned incorporation of cryptographic items into the system being acquired, and address any acquisition or testing impacts stemming from the associated certification of the items by NSA or NIST prior to connection or incorporation.

VII. IA Shortfalls: (Include as classified annex if appropriate) (Applicable to MS B, C, FRP/FDD)

A. Significant IA shortfalls

Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If applicable, identify any Acquisition Decision Memoranda that cite IA issues. If no significant issues apply, state "None".

B. Proposed solutions and/or mitigation strategies

If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall.

VIII. Policy and Guidance: (Applicable to MS A, B, C, FRP/FDD)

List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable. Capsule descriptions of the issuances are not required.

IX. Point of Contact: (Applicable to MS A, B, C, FRP/FDD)

Provide the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document. It is recommended that the system's Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.